UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/734,935	12/12/2003	Michel S. Simpson	26530.92	2224

27683 7590 10/30/2008
HAYNES AND BOONE, LLP
IP Section
2323 Victory Avenue
Suite 700
Dallas, TX 75219

EXAMINER	
LEMMA, SAMSON B	
ART UNIT	PAPER NUMBER
2432	
MAIL DATE	DELIVERY MODE
10/30/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/734,935	**Applicant(s)** SIMPSON ET AL.	
	Examiner Samson B. Lemma	**Art Unit** 2432	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 July 2008*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1 and 4-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1 and 4-21* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. This office action is in reply to an amendment filed on July 23, 2008. Independent claims 1 and 21 are amended. Claims 2-3 are previously canceled. Thus claims 1 and 4-21 are pending/examined.

Priority

2. This application does not claim priority. Therefore, the effective filling data for the subject matter defined in the pending claims of this application is **12/12/2003.**

Response to Argument

3 Applicant's remark/arguments filed on July 23, 2008 have been fully considered but they are not persuasive.

Referring to the Independent claim 1, Applicant's representative argued that the reference/s on the record, namely neither Carter nor Rider teach, suggest, or disclose the following amended limitation "**building a member definition comprising a member identifier, an access control list and a digital signature, and associating the member definition with the user."**

Applicant's representative wrote the following in support of the above argument.

"Claim 1, as amended, recites "building a member definition comprising a member identifier, an access control list and a digital signature, and

associating the member definition with the user." In contrast, neither Carter nor Rider teach, suggest, or disclose "building a member definition comprising a member identifier, an access control list and a digital signature, and associating the member definition with the user." In particular, Carter discloses that the member definition "'comprises the user identifier 48 which identifies the member to the operating system 46. The member identifier optionally includes additional information which is either provided by the user during the identifying step 114 or extracted from the appropriate user object 68, such as the user's full name, telephone number, e-mail address, or department name." (Carter, col. 13, lns 54-62). Clearly, the member definition formed by Carter does not teach a member identifier, an access control list and a digital signature.

Further, Rider does not disclose building member definitions. Instead, Rider discloses tiers of security (Rider, paragraph 35). Tier one security defines "who" can operate on a network resource and/or can access a folder or a document. (Rider, paragraph 35). Tier two security includes a set of rules for governing access based on the contents of a document. (Rider, paragraph 35). However, Rider does not disclose "building a member definition comprising a member identifier, an access control list and a digital signature, and associating the member definition with the user."

Examiner disagrees with the above argument.

The examiner counters that a careful reading of the primary reference on the record namely Carter reveals that the above argued/amended limitation or feature is indeed taught/disclosed by this reference.

Examiner would like to point out that Carter on figure 5 and on column 13, lines 52-62, and discloses the following.

“During a building step 118, **the collaborative access controller 44 builds a member definition 96 for each member of the collaborative group.** The components of each member definition 96 illustrated in FIG. 5 are formed as follows. **The member identifier 98** comprises the user identifier 48 which identifies the member to the operating system 46. The member identifier 98 optionally includes additional information which is either provided by the user during the identifying step 114 or extracted from the appropriate user object 68, such as the user's full name, telephone number, e-mail address, or department name.” Thus the above clearly meets the limitation recited as

Furthermore on column 6, lines 11-22, Carter discloses the following.

“The invention provides a computer-implemented collaborative encryption method which uses structures in the prefix portion to restrict access to the information stored in the data portion. **Users who are currently members of a collaborative group can readily access the information, while users who are not currently members of the group cannot.** Other structures in the prefix portion support **collaborative signatures, such that members of the group can digitally sign a particular version of the data portion. These collaborative signatures can then be used to advantage in ways similar to conventional individual digital signatures. For instance,**

the collaborative signatures can be used to identify the signing member."

Thus as it is shown above, and as it is clearly indicated on figure 4-6, it's undoubtedly clear that each and every limitation that is claimed is disclosed by the reference.

For clarification purpose, Examiner hereafter shows how the reference meets each and every amended limitation argued by the applicant's representative.

"**building a member definition** *[Figure 5, ref. Num "96", see "member definition"]* **comprising a member identifier** *[Figure 5, ref. Num "98", See "member identifier"*], **an access control list** *[See column 12, lines 56-57; column 13, lines 52-62, see figure 5, ref. Num 100, "encrypted document key" signed by the public key of the member. Only the member with the corresponding private key can access the document. In particular see the following which is disclosed on column 13, lines 64-column 14, lines 5, "The encrypted document key 100 is formed by encrypting the document key obtained during the step 110 with the public key of the member in question, which was obtained during the step 116. Note that the underlying document key is the same for each member of the collaborative group, but the encrypted form 100 of the document key is unique to each member. Those of skill in the art will appreciate. that the encrypted document key 100 can be decrypted only by using the private key 80 that corresponds to the public key 78 used to encrypt the document-key. "See* *also* ***"collaborative access controller 44"*** *which is described on column 6, lines 11-22 as the access controller which restrict access to the members only. Non members are restricted form accessing the information. See for instance the following disclosed on column 6, lines 11-12, "users who are currently members of a collaborative group can readily access the information, while users who are not currently members of the group cannot"]* **and a digital signature**,*[See also figure 5, ref. Num "102", "encrypted message digest", signed by the private key. In particular see what is disclosed on column 14, lines 15-21, "the encrypted message digest 102 is formed by generating a message digest based on the current contents of the data portion 94 of the document 90 and then encrypting that message digest with the private key 80 of the member who is signing the document 90." See also the abstract and column 6, lines 11-12, "collaborative signatures, such that members of the group can digitally sign a particular version of the data portion. These collaborative signatures can then be used to advantage in ways similar to conventional individual digital signatures. For instance, the collaborative signatures can be used to identify the signing member."]* **and associating the member definition with the user.** *[Figure 5 and column 6, lines 11-22, See "Users who are currently members of a collaborative group can readily access the information, while users who are not currently members of the group cannot"]*

Referring to the independent claim 11, Applicant's representative argued that, neither Carter nor Rider, teach or disclose this limitation recited as "a first member definition associated with the first data, wherein the first member definition contains a first user identifier and a first access right for a first user for the first user data". Furthermore it has been argued that any basis or indication that Carter or Rider teach or disclose this limitation is not shown.

Examiner disagrees,

For clarification purpose, Examiner hereafter shows how the reference meets each and every amended limitation argued by the applicant's representative.

a first member definition [figure 5, ref. Num "96", "Member definition "] **associated with the first data**[See figure 4, ref. Num "92"/"document "] **wherein the first member definition contains a first user identifier** [Figure 5, ref. Num "98", "member identifier"] **and a first access right for a first user for the first data** [*See column 12, lines 56-57; column 13, lines 52-62,Figure 5, ref. Num "100"; see the "encrypted document key" which is encrypted by the member's public key. Only the Member who has access to the information could use his corresponding private key to decrypt and get the document key which allows the member to access the document. In particular see the following which is disclosed on column 13, lines 64-column 14, lines 5, "The encrypted document key 100 is formed by encrypting the document key obtained during the step 110 with the* *public key of the member in question, which was obtained during the step 116. Note that the underlying document key is the same for each member of the collaborative group, but the encrypted form 100 of the document key is unique to each member. Those of skill in the art will appreciate. that the encrypted document key 100 can be decrypted only by using the private key 80 that corresponds to the public key 78 used to encrypt the document-key."] ;*

As it is indicated 14, lines 23-24 and figure 4-6, the system builds one or more member definitions. And the member definitions shown on figure 5, is associated to the documents shown on figure 4. Even though only one document is shown on figure 4, ref. Num "54, 90" the system is built for one or more documents. See the documents described on column 9, lines 35.

Thus the following is also correct.

a second member definition [figure 5, ref. Num "96", "Member definition "] **associated with the second data** [See figure 4, ref. Num "92"/"document "], **wherein the second member definition contains a second user identifier**[Figure 5, ref. Num "98"] **and a second access right for a second user for the second data;** [*[See column 12, lines 56-57; column 13, lines 52-62,Figure 5, ref. Num "100"; see the "encrypted document key" which is encrypted by the member's public key. Only the Member who has access to the information could use his corresponding private key to decrypt and get the document key which allows the member* *to access the document. In particular see the following which is disclosed on column 13, lines 64-column 14, lines 5, "The encrypted document key 100 is formed by encrypting the document key obtained during the step 110 with the public key of the member in question, which was obtained during the step 116. Note that the underlying document key is the same for each member of the collaborative group, but the encrypted form 100 of the document key is unique to each member. Those of skill in the art will appreciate. that the encrypted document key 100 can be decrypted only by using the private key 80 that corresponds to the public key 78 used to encrypt the document-key."] ;*

Referring to the independent claim 21, Applicant's representative argued that, neither Carter nor Rider, teach or disclose the amended limitation recited as "building a first member definition comprising the first access right, a first user identifier, and a first digital signature" and "building a second member definition comprising the second access right, a second user identifier, and a second digital signature."

Examiner disagrees with the above argument.

For clarification purpose, Examiner hereafter shows how the reference meets each and every amended limitation argued by the applicant's representative.

"**building a first member definition [**figure 5, ref. Num "96", "Member definition "] **comprising the first access right** [*[See column 12,lines 56-57; Figure 5, ref. Num "100"; see the "encrypted document key" which is* *encrypted by the member's public key. Only the Member who has access to the information could use his corresponding private key to decrypt and get the document key which allows the member to access the document. In particular see the following which is disclosed on column 13, lines 64-column 14, lines 5, "The encrypted document key 100 is formed by encrypting the document key obtained during the step 110 with the public key of the member in question, which was obtained during the step 116. Note that the underlying document key is the same for each member of the collaborative group, but the encrypted form 100 of the document key is unique to each member. Those of skill in the art will appreciate. that the encrypted document key 100 can be decrypted only by using the private key 80 that corresponds to the public key 78 used to encrypt the document-key." "See also "collaborative access controller 44" which is described on column 6, lines 11-22 as the access controller which restrict access to the members only. Non members are restricted form accessing the information. See for instance the following disclosed on column 6, lines 11-12, "users who are currently members of a collaborative group can readily access the information, while users who are not currently members of the group cannot"]****, a first user identifier** *[Figure 5, ref. Num "98", "Member Identifier"],* **and a first digital signature**",*[See also figure 5, ref. Num "102", "encrypted message digest", signed by the private key. In particular see what is disclosed on column 14, lines 15-21, "the encrypted message digest 102 is formed by generating a message digest based on the current contents of the data portion 94 of the document 90 and then encrypting that message digest with the private key 80 of the member who* *is signing the document 90." See also the abstract and column 6, lines 11-12, "collaborative signatures, such that members of the group can digitally sign a particular version of the data portion. These collaborative signatures can then be used to advantage in ways similar to conventional individual digital signatures. For instance, the collaborative signatures can be used to identify the signing member."]* and

As it is indicated 14, lines 23-24 and figure 4-6, the system builds one or more member definitions. And the member definitions shown on figure 5, is associated to the documents shown on figure 4. Even though only one document is shown on figure 4, ref. Num "54, 90" the system is built for one or more documents. See the documents described on column 9, lines 35.

Thus the following is also correct.

"**building a second member definition [**figure 5, ref. Num "96", "Member definition "] **comprising the second access right** [*[See column 12,lines 56-57; Figure 5, ref. Num "100"; see the "encrypted document key" which is encrypted by the member's public key. Only the Member who has access to the information could use his corresponding private key to decrypt and get the document key which allows the member to access the document. In particular see the following which is disclosed on column 13, lines 64-column 14, lines 5, "The encrypted document key 100 is formed by encrypting the document key obtained during the step 110 with the public key of the member in question, which was obtained during the* *step 116. Note that the underlying document key is the same for each member of the collaborative group, but the encrypted form 100 of the document key is unique to each member. Those of skill in the art will appreciate. that the encrypted document key 100 can be decrypted only by using the private key 80 that corresponds to the public key 78 used to encrypt the document-key." "See also "collaborative access controller 44" which is described on column 6, lines 11-22 as the access controller which restrict access to the members only. Non members are restricted form accessing the information. See for instance the following disclosed on column 6, lines 11-12, "users who are currently members of a collaborative group can readily access the information, while users who are not currently members of the group cannot"]***, a second user identifier** *[Figure 5, ref. Num "98", "Member Identifier"],* **and a second digital signature**",*[See also figure 5, ref. Num "102", "encrypted message digest", signed by the private key. In particular see what is disclosed on column 14, lines 15-21, "the encrypted message digest 102 is formed by generating a message digest based on the current contents of the data portion 94 of the document 90 and then encrypting that message digest with the private key 80 of the member who is signing the document 90." See also the abstract and column 6, lines 11-12, "collaborative signatures, such that members of the group can digitally sign a particular version of the data portion. These collaborative signatures can then be used to advantage in ways similar to conventional individual digital signatures. For instance, the collaborative signatures can be used to identify the signing member."]*

Thus for the above reasons, each and every argued limitation of the respective independent claims 1, 11 and 21 is taught by the reference/s on the record. Thus the previous rejection set forth in the previous office action is maintained.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. **Claims 1, 4-21** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Stephen R. Carter (**hereinafter referred as **Carter**)(U.S. Patent No. 5,787,175) (Date of patent 28, 1998), in view of **Rider** (hereinafter referred to as **Rider**) (U.S. Patent Publication 2006/0173999 A1) (filed on 08/07/2003, claims priority of a provisional application filed on 08/07/2002)

6. **As per independent claims 1 and 21 Carter discloses a method for controlling access to a document,** [Abstract] **comprising:**

- **Determining an access right for a user; (Column 12, lines 56-63; column 15, lines 62-67; abstract and column 8, lines 27-29)**

(Access Control Methods FIGS. 4-9 illustrate one method according to the present invention for controlling collaborative access to the work group document 90. In particular, the method includes computer-implemented steps for collaboratively encrypting the document 90 (FIG. 6) and steps for restricting access to the data portion 94 of the collaboratively encrypted document (FIG. 9)).

- **building a member definition** *[Figure 5, see "member definition"]* **comprising a member identifier** *[Figure 5, ref. Num "98", See "member identifier"]*, **an access control list** *[See column 12,lines 56-57; column 13, lines 52-62, see figure 5, ref. Num 100, "encrypted document key" signed by the public key of the member. Only the member with the corresponding private key can access the document. In particular see the following which is disclosed on column 13, lines 64-column 14, lines 5, "The encrypted document key 100 is formed by encrypting the document key obtained during the step 110 with the public key of the member in question, which was obtained during the step 116. Note that the underlying document key is the same for each member of the collaborative group, but the encrypted form 100 of the document key is unique to each member. Those of skill in the art will appreciate. that the encrypted document key 100 can be decrypted only by using the private key 80 that corresponds to the public key 78 used to encrypt the document-key. "See also "collaborative access controller 44" which is described on column 6, lines 11-22 as the access controller which restrict access to the members only. Non members are restricted form accessing the information. See for instance the following* *disclosed on column 6, lines 11-12, "users who are currently members of a collaborative group can readily access the information, while users who are not currently members of the group cannot"]* **and a digital signature**,*[See also figure 5, ref. Num "102", "encrypted message digest", signed by the private key. In particular see what is disclosed on column 14, lines 15-21, "the encrypted message digest 102 is formed by generating a message digest based on the current contents of the data portion 94 of the document 90 and then encrypting that message digest with the private key 80 of the member who is signing the document 90." See also the abstract and column 6, lines 11-12, "collaborative signatures, such that members of the group can digitally sign a particular version of the data portion. These collaborative signatures can then be used to advantage in ways similar to conventional individual digital signatures. For instance, the collaborative signatures can be used to identify the signing member."]* **and associating the member definition with the user.** *[Figure 5 and column 6, lines 11-22, See "Users who are currently members of a collaborative group can readily access the information, while users who are not currently members of the group cannot"]*

and

- **Linking the member definition to a portion of a document.**

[Figure 6, ref. Num "120"] ("Link member definition(s) with document.")

Carter does not explicitly disclose

linking the member definition to a first data portion of a document, wherein the document has the first data portion and a second data portion,

receiving a request from the user to access the document; comparing the request with the access right; and allowing access to only the first data portion in accordance with the access right

However, in the same field of endeavor, **Rider** discloses,

Linking the member definition to a first data portion of a document, wherein the document has the first data portion and a second data portion, [paragraph 0044, figure 4A & 0034-0035] *(As shown, document 400 includes descriptor portion 402 and data portion 404. Descriptor portion 402 can include basic information about the device and its operation whereas data portion 404 can include actual data, which can be employed by specific applications. Portion 406 is a portion of data 404 that has its access governed in accordance with the principles of tier two security as described herein. That is,* ***one or more access rights can be associated with portion 406****. Although one portion 406 is shown, an ordinarily skilled artisan will appreciate that the same or other access rights can govern other portions of data portion 404.)*

Receiving a request from the user to access the document; comparing the request with the access right; and allowing access to only the first data portion in accordance with the access right [Paragraph 0034-0035 paragraph 0044, figure 4A] *(On paragraph 0034, the following has been disclose. Moreover, security manager 170 can* *permit, restrict or completely deny a user* ***request to access one or more documents*** *as well as the contents of those documents. A document or a portion thereof can represent a command for, or a configuration of, one of devices 135 such as a router or switch. Security manager 170 governs by determining whether a particular user has access rights to a specific network resource,* ***a particular document or only a portion of a document. Furthermore on paragraph 0035, the following has been disclosed. "****By restricting access in relation to a document's content, a more fine-grained approach to configuring, managing and monitoring network resources is realized. Hence, tier two security restricts a user to data* ***constituting a portion of an entire document rather than providing complete or no access to that document.*** *For example, FIG. 4A depicts* ***document portion 406 that is accessible. Note that other portions of document 400 are not necessarily accessible to that user.")***

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the feature such as linking the member definition to a first data portion of a document, wherein the document has the first data portion and a second data portion and receiving a request from the user to access the document; comparing the request with the access right; and allowing access to only the first data portion in accordance with the access right as per teachings of **Rider** into the method as taught by **Carter**, in order to provide a more fine-grained access control to the resources (portions of documents) [*See For instance Rider on paragraph 0035]*

7. **As per independent claim 11 Carter discloses a method for controlling access to a document,** [Abstract] **comprising:**

- **A document comprising a first data and a second data.**[*"the documents, which are indicated as 4, ref. Num "92" could be more than one as it is indicated on column* ***14, lines 23-24 and figure 4-6, the system builds one or more member definitions which is associated with one or more documents.]***

a first member definition [figure 5, ref. Num "96", "Member definition "] **associated with the first data**[See figure 4, ref. Num "92"/"document "] **wherein the first member definition contains a first user identifier** [Figure 5, ref. Num "98"] **and a first access right for a first user for the first data** [*Figure 5, ref. Num "100"; see the "encrypted document key" which is encrypted by the member's public key. Only the Member who has access to the information could use his corresponding private key to decrypt and get the document key which allows the member to access the document. In particular see the following which is disclosed on column 13, lines 64-column 14, lines 5, "The encrypted document key 100 is formed by encrypting the document key obtained during the step 110 with the public key of the member in question, which was obtained during the step 116. Note that the underlying document key is the same for each member of the collaborative group, but the encrypted form 100 of the document key is unique to each member. Those of skill in the art will appreciate. that the encrypted document key 100 can be decrypted only by using the private* *key 80 that corresponds to the public key 78 used to encrypt the document-key."] ;*

As it is indicated 14, lines 23-24 and figure 4-6, the system builds one or more member definitions. And the member definitions shown on figure 5, is associated to the documents shown on figure 4. Even though only one document is shown on figure 4, ref. Num "54, 90" the system is built for one or more documents. See the documents described on column 9, lines 35.

Thus the following is also correct.

a second member definition [figure 5, ref. Num "96", "Member definition "] **associated with the second data** [See figure 4, ref. Num "92"/"document "], **wherein the second member definition contains a second user identifier**[Figure 5, ref. Num "98"] **and a second access right for a second user for the second data;** [*Figure 5, ref. Num "100"; see the "encrypted document key" which is encrypted by the member's public key. Only the Member who has access to the information could use his corresponding private key to decrypt and get the document key which allows the member to access the document. In particular see the following which is disclosed on column 13, lines 64-column 14, lines 5, "The encrypted document key 100 is formed by encrypting the document key obtained during the step 110 with the public key of the member in question, which was obtained during the step 116. Note that the underlying document key is the same for each member of the collaborative* *group, but the encrypted form 100 of the document key is unique to each member. Those of skill in the art will appreciate. that the encrypted document key 100 can be decrypted only by using the private key 80 that corresponds to the public key 78 used to encrypt the document-key."] ;*

Carter does not explicitly disclose

Wherein the document has the first data portion and a second data portion,
receiving a request from the user to access the document; comparing the request with the access right; and allowing access to only the first data portion in accordance with the access right

However, in the same field of endeavor, **Rider** discloses,

Linking the member definition to a first data portion of a document, wherein the document has the first data portion and a second data portion, [paragraph 0044, figure 4A & 0034-0035] *(As shown, document 400 includes descriptor portion 402 and data portion 404. Descriptor portion 402 can include basic information about the device and its operation whereas data portion 404 can include actual data, which can be employed by specific applications. Portion 406 is a portion of data 404 that has its access governed in accordance with the principles of tier two security as described herein. That is,* ***one or more access rights can be associated with portion 406****. Although one portion 406 is shown, an ordinarily skilled artisan will appreciate that the same or other access rights can govern other portions of data portion 404.)*

Receiving a request from the user to access the document; comparing the request with the access right; and allowing access to only the first data portion in accordance with the access right [Paragraph 0034-0035 paragraph 0044, figure 4A] *(On paragraph 0034, the following has been disclose. Moreover, security manager 170 can permit, restrict or completely deny a user* ***request to access one or more documents*** *as well as the contents of those documents. A document or a portion thereof can represent a command for, or a configuration of, one of devices 135 such as a router or switch. Security manager 170 governs by determining whether a particular user has access rights to a specific network resource,* ***a particular document or only a portion of a document. Furthermore on paragraph 0035, the following has been disclosed. "****By restricting access in relation to a document's content, a more fine-grained approach to configuring, managing and monitoring network resources is realized. Hence, tier two security restricts a user to data* ***constituting a portion of an entire document rather than providing complete or no access to that document.*** *For example, FIG. 4A depicts* ***document portion 406 that is accessible. Note that other portions of document 400 are not necessarily accessible to that user.")***

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the feature such as linking the member definition to a first data portion of a document, wherein the document has the first data portion and a second data portion and receiving a request from the user to access the document; comparing the request with the access right; and allowing access to only the first data portion in accordance with the access right as per teachings of **Rider** into the method as taught by **Carter**, in order to provide a more fine-grained access control to the resources (portions of documents) [*See For instance Rider on paragraph 0035].*

8. **<u>As per claim 4 the combination of Carter and Rider</u> discloses a method as applied to claims above. Furthermore, Carter discloses the method, further comprising adding a new user to the document**.*[Figure 7, column 7, lines 3-5] ("adding a new member")*

9. **<u>As per claim 5 the combination of Carter and Rider</u> discloses a method as applied to claims above. Furthermore, Carter discloses the method, further comprising removing a member from the document.** *[Figure 8, column 7, lines 5-7] ("removing a member")*

10. **<u>As per claims 6 and 15 the combination of Carter and Rider</u> discloses a method as applied to claims above. Furthermore, Carter discloses the method further comprising: storing the member definition remotely from the document.** *[column 14, lines 35-38]*

11. **<u>As per claims 7 and 16 the combination of Carter and Rider</u> discloses a method as applied to claims above. Furthermore, Carter discloses the method further comprising: storing the member definition in the document.** *[Column 14, lines 31-34] ("In one embodiment, linking is accomplished by <u>storing</u> the encrypted data portion 94 and the prefix portion 92 (including one or more <u>member definitions</u> 96) together in a file on a disk, tape, or other conventional <u>storage</u> medium.")*

12. **As per claim 8 the combination of Carter and Rider discloses a method as applied to claims above. Furthermore, Carter discloses the method further comprising: further comprising:**
encrypting the document; and linking the member definition with a public key and a private key.*[column 11, lines 61- column 12, lines 7]*

13. **As per claims 9-10 and 12-13 the combination of Carter and Rider** discloses a method as applied to claims above. Furthermore, Rider discloses the method, further comprising: determining a second access right for the user; building a second member definition using the second access right; and linking the second member definition to a second portion of a document[Paragraph 0034-0035 paragraph 0044, figure 4A].

14. **As per claim 14 the combination of Carter and Rider discloses a method as applied to claims above. Furthermore, Carter discloses the method wherein the first member definition contains a digital signature.** *[Abstract and figure 10, ref. Num "184"]*

15. **As per claims 17-20 the combination of Carter and Rider discloses a method as applied to claims above. Furthermore, Carter discloses the method wherein the document is tagged document/XML document/text document/binary document.** *[Column 9, lines 32-61]*

Conclusion

16. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am---4: 30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

10/15/2008

/Samson B Lemma/

Examiner, Art Unit 2432

/Gilberto Barron Jr/

Supervisory Patent Examiner, Art Unit 2432

Application Number	Application/Control No. 10/734,935	Applicant(s)/Patent under Reexamination SIMPSON ET AL.	
	Examiner Samson B. Lemma	Art Unit 2432	